Avionics/Intelligence and Electronic Warfare Bulletin

"Serving the Needs of the Army's A/IEW Community"

Volume 2, Issue 1 **July 2001**

The All Source Analysis System (ASAS) Family of Systems: Providing Operational Intelligence to the Warfighter

Introduction

Army operational forces are equipped and trained to respond to an ever-changing and complex array of threats to our national interests. The ASAS family of systems provides soldiers with a flexible set of system tools that enable the analysis, processing, display, and dissemination of intelligence information related to these threats. Collectively, this suite of systems links intelligence functional area activities and organizations, from the national to the tactical level, in a flexible and complementary manner to provide the Warfighter with near real-time processed intelligence information.

The U.S. Army Communications-Electronics Command (CECOM), Software Engineering Center (SEC), Intelligence Fusion Systems (IFS) Branch provides Post Production Software Support (PPSS) for ASAS. The rapid advance of technology, the emphasis on joint warfighting, and the constant evolution of the threat that our soldiers face are all factors that impact evolving intelligence requirements. ASAS must also evolve to provide support to the intelligence mission area. CECOM SEC IFS coordinates closely with user representatives to maintain these systems and provide for near-term software enhancements to the ASAS family of systems that enable them to keep pace with the dynamic face of the threat. This dynamic approach to PPSS serves to provide for a family of intelligence systems that support the operational commander's requirement for battlefield situational awareness.

The ASAS family of systems is composed of the ASAS-All Source (ASAS-AS), the ASAS-Single Source (ASAS-SS), the ASAS-Remote Workstation (ASAS-RWS), ASAS-Light (ASAS-L), and the ASAS-Communications Control Set (ASAS-CCS). This family of systems is employed at different echelons and designed to perform functions that collectively enable soldiers at all echelons to provide commanders with a view of the enemy threat. This

(cont'd page 3)

In This Issue

The "Avionics/Intelligence and Electronic Warfare Bulletin" is a quarterly professional periodical published by the CECOM SEC Avionics/Intelligence and Electronic Warfare Division

From the Senior Editor's Desk

Written by Mr. Joseph Ingrao, A/IEW Division Chief

High-Tech Army

The Army is facing a unique challenge as it attempts to infuse high technology into the battlefield environment. As we attempt to insert leading-edge technologies, an environment of disorder and informality occurs. In order to avoid chaos and ensure continuity, certain themes must be followed.

Consistent Priorities

A technology focus must be maintained over extended periods of time. These consistent priorities should be strongly focused by top Army management.

Adaptability

Although we must have a well-defined focus, we must balance it with the willingness, and the will, to undertake major and rapid change when necessary. Concentration, in short, does not mean stagnation. Immobility is the most dangerous behavioral pattern a high-tech Army can develop.

Organizational Cohesion

The key to success for a high-tech Army is not simply periodic renewal. There must also be cooperation in the translation of new ideas into new products and processes. If we have the driving function, the most important success factor is the ability to integrate. It's also the most difficult part of the task. To succeed, the energy and creativity of the whole Army must be tapped. Anything that restricts the flow of ideas or undermines the trust, respect, and sense of commonality of purpose among individuals is a potential danger.

ASAS (cont'd)

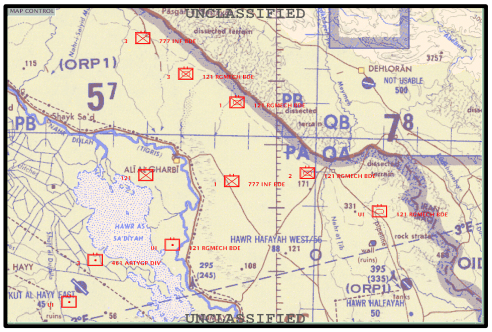
information is provided to other systems within the Army Battlefield Command System (ABCS) and joint systems, such as the Global Command and Control System (GCCS), and then merged with friendly unit information to form the Common Operating Picture (COP). The following paragraphs briefly describe the role that each of these systems plays within the intelligence mission area and depicts CECOM SEC IFS efforts to address soldiers' near-term requirements. Near-term efforts are coordinated among Team ASAS members, the Training and Doctrine Center (TRADOC) System Manager (TSM) ASAS, Project Manager Intelligence Fusion Systems (PM Intel Fusion), and CECOM SEC IFS to ensure that both the near-term and longer-term developmental efforts are supportive in nature.

ASAS Family of Systems Common Functions

Although each ASAS system is designed to support specific operational requirements, there are common functional threads or capabilities that enable each system to display, exchange, and store information. Each system is capable of receiving formatted information and automatically parsing that information into a database. ASAS users are able to plot information from stored records and to develop user-definable views of the information. The operators, through the use of database queries, develop these different views. ASAS users can view selected information elements based upon parameters that they define. For example, if a commander were facing an armored force and knew that enemy tactics included focusing tank forces at the point of the main attack, a query could be designed to view/display the position of known enemy tank forces only. The result of this user-defined query could be viewed independently from other enemy information in the database and provide the commander with a clear picture of the position of enemy tank units. ASAS also provides the capability to alert the operator to the receipt of specific information via audible or visual alarm. Referring back to the previous example, the operator could designate an alert based upon any movement of enemy tank forces within a geographic sector. The operational commander could then target these forces to prevent attack or in support of a counterattack. These common functions contribute to providing operational users of ASAS the capability to establish the most up-to-date and accurate array of threat forces on the battlefield. Specific system functionality and roles are outlined in the paragraphs below.

ASAS-AS

The ASAS-AS provides for the collection, analysis, and dissemination of multi-intelligence products. The ASAS-AS serves as the operational link to the national Modernized Integrated Database (MIDB) and provides for the capability to fuse intelligence information across disciplines and echelons. The key enabler to this process is the All Source Correlated Database (ASCDB). The ASCDB serves as a centralized repository of information records that can be added, updated, and viewed based upon user requirements. The External Database Coordination (EDC) message is the information



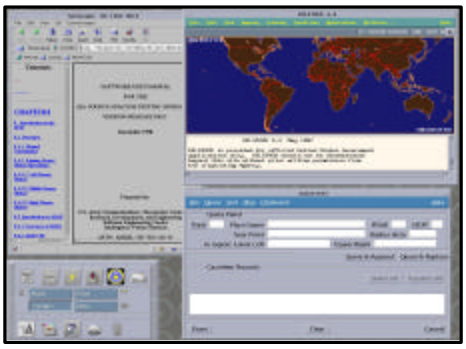
(cont'd next page)

ASAS (cont'd)

exchange vehicle employed by ASAS to pass ASCDB information. The ASAS-AS can tailor the information contained in the EDC messages based upon user-defined requirements and provide recurring updates to ensure that ASAS family of system databases are current and consistent. The Military Intelligence (MI) Brigade (Bde) provides ASAS-AS support to the Analysis and Control Element (ACE). Near-term PPSS efforts to enhance ASAS-AS functionality are focused toward providing soldiers with the capability to visualize the situations faced during Stability and Support Operations (SASO). The SASO environment requires the ability of the system to store, process, display, and disseminate Individual, Event, and Organization (IE&O) the information that is required for analysis of unique operational situations.

ASAS-SS

The ASAS-SS system is designed to provide the commander with processed Signals Intelligence (SIGINT). SIGINT consists of correlated Electronic Intelligence (ELINT) and Communications Intelligence (COMINT) information. SIGINT information provides commanders with an electronic enemy picture of the battlefield that is provided to the ASAS-AS, which incorporates the information into the ASCDB to display the overall situation. The MI Bde provides the ASAS-SS enclave to designated Army operational units. Near-term PPSS enhancements to the ASAS-SS are focused toward the enhancement of the map application and addition of the distributive collaborative planning product InfoWorkSpace (IWS). The addition of the IWS client to the ASAS-SS software baseline will provide users with a distributed collaborative planning capability via Joint Intelligence Virtual Architecture (JIVA) servers that have been established on the Joint Worldwide Intelligence Communication System (JWICS) network. A communication enhancement to the ASAS-SS is being prototyped to interface with the Integrated Broadcast Services (IBS) via the Joint Tactical Terminal (JTT).



ASAS-CCS

The ASAS-CCS serves as the primary message processing system for the ASAS family of systems. The ASAS-CCS is specifically designed to enable information exchanges between ACE systems operating at the TS/SCI level and the majority of ABCS consumers that operate at the SECRET Collateral security level. The ASAS-CCS is composed of a Tactical Communications Support Processor (TCSP) and a Secure Messaging and Routing Terminal (SMART). The TSCP is both a store and a forward, formatted message switch that allows ACE ASAS systems to send and receive formatted messages via either the TS/SCI Defense Special Security Communications System (DSSCS) or SECRET Collateral (Automated Digital Network (AUTODIN) networks. The SMART enables SECRET Collateral level Local Area Network (LAN) connectivity between the ACE and the Collateral ASAS-RWS by serving as a security firewall. The SMART provides connectivity to Secure Internet Protocol Router Network (SIPRNET) and Mobile Subscriber Equipment (MSE) Tactical Packet Network (TPN) communication paths. The ASAS-CCS can be found at MI Bde units supporting ACEs

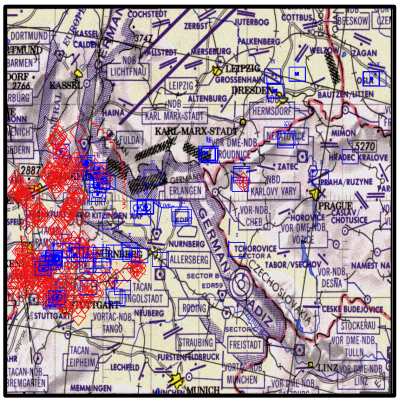
(cont'd next page)

ASAS (cont'd)

(at the division level or above) in either shelterized or transit case configurations. Although the TCSP supports the accredited processing and exchange of formatted messages between the ASAS-AS and Collateral ABCS systems, currently there is no methodology for supporting LAN connectivity between the TS/SCI ACE and collateral ABCS. A PM Intel Fusion initiative that will enable multi-level connectivity is the Trusted Workstation (TWS). The TWS, when fielded, will support the exchange of LAN (e-mail) traffic between networks operating at dissimilar security classification levels.

ASAS-RWS and ASAS-L

The ASAS-RWS is the information fusion system component of ABCS. The ASAS-RWS provides the staff intelligence officer at echelons Bde and above with analytical tools that support the operational commander's Intelligence Preparation of the Battlefield (IPB) and Situational Awareness requirements. The ASAS-RWS is typically connected to the Tactical Operations Center (TOC) LAN, and system functionality is focused toward providing operationally relevant, processed intelligence to the Warfighters. IPB tools support production of the Modified Combined Obstacle Overlay (MCOO) and assist staff officers in the analysis of potential enemy courses of action. The ASAS-RWS receives the EDC message from the ASAS-AS and uses this information, along with locally gathered intelligence, to maintain the most recent enemy picture for the local commander. CECOM SEC IFS supports both Block I and Block II variants of the ASAS-RWS. Both of these ASAS-RWS systems possess similar functionality but the Block II system was designed in a modular fashion to conform to the Defense Information Infrastructure Common Operating Environment (DII COE).



DII COE compliance facilitates the use of common software modules, such as the Joint Mapping Tool Kit (JMTK). The ASAS-L is hosted on a ruggedized laptop and effectively extends selected ASAS-RWS functionality down to the battalion level. The ASAS-L receives the EDC message from the ASAS-RWS at Bde and provides for extension of a CIP to the battalion level. Near-term enhancements to the ASAS-RWS include enhanced IE&O processing and implementation of distributed collaborative planning client software. CECOM SEC IFS recently began the transition efforts that will lead to CECOM SEC IFS assuming PPSS responsibilities for the ASAS-L.

Summary

This article provides a short overview of the systems that compose the currently fielded ASAS family of systems. These systems provide operational commanders at Echelons Above Corps (EAC) down to the maneuver battalion with up-to-date and accurate pictures of enemy forces. This view is provided to ABCS and joint systems and merged into a COP that provides Warfighters with an understanding of the position of

(cont'd next page)

ASAS (cont'd)

friendly and enemy forces on the battlefield. The result is a common situational awareness that facilitates a rapid decision-making process during high tempo operations. CECOM SEC IFS, as a member of Team ASAS, provides for the maintenance and near-term enhancements to these systems to meet evolving battlefield requirements. CECOM SEC IFS support includes both depot-level maintenance of system software baselines and on-site support to the soldiers operating ASAS through regional Field Software Services Support (FSSS) representatives. Through close and continuous interaction with ASAS users and their representatives CECOM SEC IFS aggressively pursues the maintenance and enhancement of ASAS to meet the needs of our Warfighters.

United States Army Communications-Electronics Command
Software Engineering Center Intelligence Fusion Systems
Fort Huachuca, Arizona 85613-5000
Phone (520) 538-6188; DSN 879-6188
http://cecom-ifs.army.mil

Submitted by Mr. Stu Brock, ILEX Systems, CECOM SEC IFS

TRAILBLAZER Software Improvements Support U.S. and Allied Efforts

Two recent modifications, explained below, to the AN/TSQ-138A TRAILBLAZER show the Army's commitment to this valuable intelligence system. The first modification will help current U.S. Army users during their daily operations, and the second will potentially allow U.S. Allies to incorporate the system into their intelligence architectures.

Operators Receive Help System with V2.0d Release

The CECOM Software Engineering Center (SEC), Ft. Monmouth, successfully fielded a TRAILBLAZER software release that provides system operators with an on-line Help System containing general and context-sensitive help screens. The Help System implements a common format normally seen in PC-based applications, providing "Contents," "Index," and "Find" capabilities, as well as hyper-links throughout the individual screens. The "Help" matter presented consists of information and data contained in the TRAILBLAZER Operator Manual, TM 32-5895-500-10. The software upgrade was tested extensively at the CECOM SEC Life Cycle Software Support Center (LCSSC), and subsequently using the systems and the assistance of the soldiers assigned to the 305th MI Battalion (Bn), Ft. Huachuca, AZ. The software release package has been shipped and is now in the hands of the soldiers at the 312th MI Bn, 102nd MI Bn, 103rd MI Bn, and the 304th MI Bn.

TRAILBLAZER Modified For Foreign Military Sales

Working with the CECOM Security Assistance Management Directorate (SAMD), the CECOM SEC recommended and implemented software changes to the operational software of the AN/TSQ-138

(cont'd next page)

TRAILBLAZER (cont'd)

TRAILBLAZER system to satisfy export requirements mandated by other Government agencies. These changes were made without affecting the accuracy or basic capabilities of the system. Thorough testing of the FMS software was accomplished at the CECOM SEC LCSSC using the resident Operational Mock Up (OMU) and subsequently with a targeted FMS system on loan from the Tobyhanna Army Depot interoperating with the LCSSC-resident AN/TRQ-32A(V)2 TEAMMATE and AN/TSQ-175 TIGER systems. Final system testing was conducted at the Tobyhanna Army Depot using the three systems destined for the FMS Customer.

Submitted by Mr. David Leciston, CECOM SEC

Shortstop Electronic Protection System

Thanks to the Shortstop Electronic Protection System (SEPS), troops and high value assets, such as light-armored vehicles and light weight, highly mobile military transports and platforms, have an "invisible electronic umbrella" that detects and pre-detonates enemy artillery and mortar shells, with electronic proximity fuses, at a safe distance or safe Height-of-Burst (HOB). The deployment of SEPS in Bosnia and Operation Desert Storm and Shield is testimony of SEPS's ability to protect our troops and high value assets.

"The Army's Shortstop System will provide our soldiers in Bosnia with an added level of security that was never dreamed possible should they come under artillery fire," said MG David Gust, Program Executive Officer for Intelligence and Electronic Warfare (IEW).

Proximity fuses are programmed to explode several feet above the ground to gain maximum damage and successful lethal strikes. They transmit and receive electronic signals to successfully perform their missions. SEPS is an Electronic Countermeasure (ECM) System that creates an electronic field to trick proximity fuses into safely detonating hundreds of meters away from their target. SEPS uses software-controlled signal detection, recognition, identification and classification techniques, as well as control algorithms to successfully protect our troops and high value assets.

Packaged in a suitcase-sized enclosure weighing approximately 25 pounds, SEPS can be activated and operational within seconds. It can easily be transported as a stand-alone unit, man-pack, or vehicle-mounted. Its passive electronics and operational features make SEPS impervious to detection by enemy signal intelligence sensors.

(cont'd next page)

Shortstop (cont'd)

AN/GLQ-16
STANDALONE

AN/VLQ-11
VEHICLE MOUNT

AN/PLQ-7
MANPACK

The ability of SEPS, however, to successfully perform its mission is highly dependent on the system software's ability to continuously perform as required and to provide effective ECM. As deployed SEPS units become battlefield weary and are increasingly used, the system software encounters performance degradation and requires diagnostics to fully recover effective performance. Additionally, as new enemy fuse threats emerge and get smarter, such as employing Electronic Counter Countermeasures (ECCM), the system software must be maintained to counter these new challenges.

To maintain the SEPS system software's ability to perform and provide effective ECM, the CECOM Software Engineering Center (SEC) provides Life Cycle Software Support Services (LCSSS) for SEPS. LCSSS is defined as the overall software system support necessary to develop, sustain, modify, refine, and improve software, including computer code, data, documentation, and all other support software and hardware elements.

The SEC SEPS Integrated Product Team (IPT) provides LCSSS including activities such as, (1) independent review and evaluation of draft and final SEPS documentation for completeness and compliance with software engineering principles and practices, as well as for consistency, accuracy and traceability; (2) active participation at SEPS software demonstrations; and (3) review and analysis of SEPS plans and procedures submitted by the SEPS developer in advance of acceptance testing, including verification of adequate testing of baseline requirements. These services include citing deficiencies, making recommendations for corrective action, and assisting the customer in resolving technical problems.

SEPS IPT major highlights and accomplishments include, (1) resolving communication polling for 1553 Data Recording Software; (2) actively participating at Functional Qualification Tests (FQT) at remote SEPS development and test facilities; and (3) participating in Live Fire Testing, including review and assessment of the test data.

SEC will be establishing, operating, and maintaining the SEPS Post Production Software Support (PPSS) Environment, including the acquisition of hardware, test equipment, software and software tools, and software configuration management.

(cont'd next page)

Shortstop (cont'd)

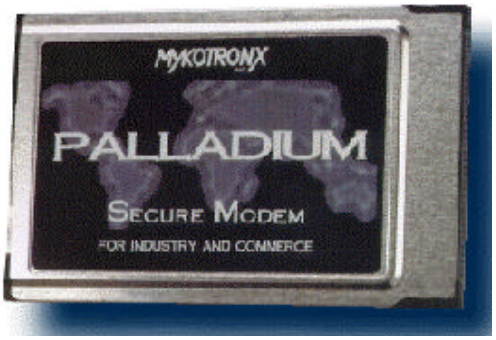
SEC also provides Software Engineering Services and Support for the development of software tools, modification of SEPS code, and the implementation, test and documentation of those tools and required code modifications. Software tool development and code modification includes the expansion of SEPS to protect troops and high value assets from new and emerging categories or behaviors of electronically fused munitions.

"While it is our hope that American forces do not come under attack, based on extensive testing against many types of proximity fused weapons, we have confidence in the ability of the Shortstop System to defeat attack," said MG Gust. And, with the provision of SEPS LCSES from SEC, this confidence will continue today and into the future.

Submitted by Mr. Kwok Lo, CECOM SEC ECB

Palladium Modem in Approval Stage to Become Catalyst for Improved ARAT SIPRNET Dial-Up Connectivity

The Electronic Combat Branch (ECB) Chief has approved the addition of the Palladium Secure Modem product as a dial-up method to the ARAT Secure Internet Protocol Router Network (SIPRNET) communications infrastructure. Currently, ARAT is awaiting approval from the CECOM G-6 office and SEC Designated Accreditation Authority. For those of you not familiar with the Palladium Modem, this article will offer an introduction to the product and its capabilities.



For those of us that remember the Palladium element from chemistry class, it was a silver-white metallic chemical element used as a catalyst and in alloys. Those of us supporting ARAT are hoping the future approval and addition of the Palladium Modem service will act as a catalyst in providing Electronic Warfare Officers (EWOs) another option for dependable SIPRNET data connectivity to mission critical data. The Palladium Secure Modem is a 33.6 Kilobytes per second (Kbps) data modem with an on-board cryptographic processor providing tamper-resistant, high-assurance secure communications.

The Palladium features two modes of operation - for ARAT communication purposes we will require the Palladium be used in the "Secure Modem Mode," where the modem acts as a V.34 modem, providing secure data communications over standard, analog telephone lines. It supports a variety of modem standards, in addition to V.34, for compatibility with older telecommunication infrastructures. The V.42 and MNP™ level 2–4 protocols ensure error-free data transmission. In the FORTEZZA® Mode, the Palladium functions as a FORTEZZA® Crypto CARD, supporting the full range of cryptographic algorithms. In either mode, the Palladium requires the user to enter the proper personal identification number (PIN) prior to use.

(cont'd next page)

Palladium (cont'd)

The Palladium modem has been approved by the National Security Agency (NSA) as a dial-up method for data transfer, up to the SECRET classification, and is FIPS 140-1 Level 1 certified. The Defense Information Systems Agency (DISA) has accredited the ARAT as a dial-up device to the SIPRNET. Currently, the Palladium is being used by many Army organizations, including EUCOM, SOUTHCOM, CENTCOM, JSOC, SOCOM, and USASOC to name a few. In fact, the Chief of Staff for the Army, General Shinseki is also using the Palladium secure modem. The ARAT SIPRNET dial-up capabilities enable EWOs to download mission critical data that the ARAT and the ECB create for the Army Target Sensing System (ATSS) community. The Palladium modem will allow the ARAT to offer an alternate means of secure dial-up connectivity for the EWO community, thus allowing the ATSS users, at all echelons, the ability to access pertinent reprogramming information and updated software into garrison and tactical locations.

The cryptological "fill" for the Palladium is on the card when ordered; it simply needs to have a certificate loaded by a Certificate Authority. This is done in the same manner, and by the same equipment, as a FORTEZZA® card to be used for DMS. Another advantage is that the Palladium card is unclassified. The only time it becomes classified is when it has been loaded with a Secret-level certificate and the user enters the PIN. Upon power down, or card removal, it is unclassified again until the PIN is entered.

The Palladium is a PCMCIA type 2 device that is designed to work in the PCMCIA adapter slot of your laptop computer. Advantages of using the Palladium modem for your secure point-to-point protocol (PPP) dial-up connections include its speed over the analog Public Switched Telephone Network (PSTN) and its user friendliness. With a top connection speed of 33.6 Kbps, it has a speed advantage over the STU-III (normally 9.6 Kbps) and the STE (9.6 Kbps on the PSTN). The Palladium also incorporates much better error correction capabilities than the STU-III and will furnish better results on DSN. In fact, NSA has tested the Palladium's performance in numerous CONUS and OCONUS locations using both commercial and DSN lines, with very impressive results. The Palladium is very user friendly, and is similar in use to a normal PCMCIA modem used to dial into the Internet.

It should be noted, however, that Palladium modems will only talk to other Palladium modems (there is a FORTEZZA® modem protocol and the Palladium will talk to any other modem that follows this protocol). A Palladium user can only communicate to another Palladium if authentication is achieved through the successful exchange and verification of Key Material Identification (KMID) information stored on each Palladium. If the KMID information of the "calling" Palladium is not included in the access control list of the "called" Palladium, and vice versa, the connection will fail. Also, the Palladium is not currently compatible with STU/STE technology. A Palladium user will only be able to perform secure data transfer and has no capability to do secure voice, as with a voice STE.

A Palladium modem, with all the software needed to make it operational, will cost the user around $900. Currently the Palladium is a sole source product, and can be ordered through Kasten Chase Corporation. ARAT, however, is trying to gain accreditation from CECOM to incorporate this technology, as well as the STE, in our suite of dial-up methods.

(cont'd next page)

Palladium (cont'd)

If the approval of the Palladium addition is granted by CECOM, the device will become an additional dial-up method to ARAT's SIPRNET dial-up server located in the Rapid Reprogramming Communication Infrastructure Laboratory, (R^2CIL), Bldg. 1210, Ft. Monmouth, NJ. With the addition of the Palladium and STE, ARAT's R^2CIL will offer three dial-up methods (STU-III, STE and Palladium) to ARAT SIPRNET services and a link to the Multi-Service Electronic Warfare Data Distribution System (MSEWDDS). One final note - there are background efforts commencing at Eglin AFB to also offer the Palladium and STE as direct dial-up options to the MSEWDDS. The STE is capable of encrypted data transfer up to 128 Kbps on an ISDN line. When connected to the PSTN, the STE is also capable of emulating STU-IIIs with a data rate of 9.6 Kbps. If you currently have an STE, you are capable of dialing into the ARAT STU-III bank at the 9.6 Kbps rate.

ARAT was expecting to have the Palladium Modem Communication Servers (OPtiva Servers) fully installed and operational within the R^2CIL by late Spring 2001. However, the accreditation of the addition of the Palladium and STE will take longer than originally anticipated, therefore, there is currently no definite availability date. The ARAT team is fully prepared to install and configure the Optiva Servers and Palladium modems once official accreditation approval is received. The OPtiva Server will be compatible with most third-party client software, such as Dial-Up Networking included with Windows 95, Windows 98 and Windows NT. OPtiva's implementation of asynchronous PPP is compatible with industry-leading TCP/IP software and has been tested with the most popular TCP/IP clients. There will be additional articles concerning the Palladium in future issues of the *A/IEW Bulletin* giving the details concerning the Palladium approval, ordering information, usage and configuration when establishing connectivity to ARAT SIPRNET Servers. For those that are interested in ARAT gaining the Palladium and STE dial-up capability to our ARAT SIPRNET servers, please send correspondence to:

U.S. Army CECOM
Software Engineering Center
ATTN: AMSEL-SE-WS-AI
Fort Monmouth, NJ 07703
FAX: 732-532-5239/992-4238 (DSN)

Alternatively, email: arat@arat.iew.sed.monmouth.army.mil

Receiving responses outlining the need for improved dial-up connectivity from our warfighter customers is invaluable in assisting us in gaining the accreditation approval we need to incorporate this technology in a timely fashion. ARAT is very confident that the addition of the Palladium modem and STE will be extremely beneficial in supplying superior dial-up connectivity to our customers. For those with general or performance data questions concerning the Palladium Modem, the ARAT Support team can be contacted at 732-532-9395/DSN: 992-9395.

Submitted by Mr. Michael Crapanzano, ILEX Systems

New Technologies on the Horizon for Access to ARAT

The Army Reprogramming Analysis Team (ARAT) recently attended the Information Assurance Solutions Working Symposium (IASWS) in New Orleans, LA. The symposium covered many of the new technologies on the horizon that will be utilized by DoD to access information. These technologies will help increase access speeds and reliability of the connections, as well as provide the information security needed for accessing the Secure Internet Protocol Router Network (SIPRNET). ARAT will be investigating and testing some of these technologies to make access easier for the Warfighter. These technologies include:

- Secure Terminal Equipment (STE) via analog phone line
- STE via Integrated Services Digital Network (ISDN)
- Palladium Secure Modem
- OMNI™ Secure Terminal

The L-3 Communications Corp. STE is currently replacing the Secure Telephone Unit Type III (STU-III) telephones throughout DoD, and will become the primary voice and data communications device for DoD. The STE is basically the same as a STU-III, but with far more capabilities. The STE terminals are available in four configurations:

- The Office STE Terminal provides access to ISDN and Public Switched Telephone Network (PSTN) telecommunications systems.
- STE Remote Controllable Secure Voice/Data Terminal (STE-R). STE-R is both digital and analog, allowing backward compatibility with the STU-III.
- Data STE, which provides data only connections via ISDN and PSTN telecommunications systems.
- The Tactical STE Terminal provides access to ISDN, PSTN, TRI Service TACtical network (TRI-TAC), and serial EIA-530A/EIA-232 Black Digital Interface (BDI) telecommunications systems.

The Office and Tactical STE Terminals provide:

- Non-secure voice telephone service interoperable with conventional ISDN and PSTN telephones, STE and STU-III terminals, and Digital Non-Secure Voice Terminals (DNVT).
- Secure voice interoperable with other STE or STU-III Terminals.
- Secure facsimile interoperable with units supported by other STEs or STU-III Terminals, and
- Secure data interoperable with terminals supported by STEs or STU-III Terminals.

(cont'd next page)

New Technologies (cont'd)

As it pertains to the ARAT, STE access procedures will be very similar to STU-III access. If a user currently has a STE, that user can dial in just as if dialing in using a STU-III; the same access numbers will work for the STE that work for the STU-III. ARAT has done some testing and configuring of STEs, and will produce a configuration and procedures help guide in the future. As it stands, there are very few differences in the configuration or procedures for using a STE as opposed to using a STU-III. Some of the biggest differences in utilizing a STE are the data speeds. When utilizing a STE on an analog phone line (PSTN), the maximum data speed, which a user can access the ARAT SIPRNET dial-up, is 9.6 Kilobytes per second (Kbps). This is the same as an AT&T 1100 STU-III. It is slightly slower than an AT&T 1910 STU-III, which can access the ARAT SIPRNET network at 38.4 Kbps. This 38.4 Kbps access is currently configured for two of ARAT's dial-in access phone numbers.

ARAT is currently in the process of obtaining one ISDN line for dial-up access. This will allow a user on ISDN to dial into the network at speeds of up to 128 Kbps. This will provide a user with a very fast and reliable connection. ARAT will notify users when this service is available and of all its associated configurations and procedures.

ARAT is also exploring the use of the Palladium Secure Modem. The Palladium Secure Modem is a 33.6 Kbps modem with an on-board cryptographic processor. The Palladium is a PCMCIA type 2 device, and is very similar to a standard PCMCIA modem you would use in a laptop and is basically just as easy to use. For more information on the Palladium Secure Modem, read the article "Palladium Modem To Become Catalyst for Improved ARAT SIPRNET Dial Up Connectivity", written by Mr. Michael Crapanzano, ILEX Systems, also in this issue of the *A/IEW Bulletin.*

Another technology being explored by the ARAT is the L-3 Communications Corp. OMNI™ Secure Terminal. The standard OMNI™ adds Type-I security to any commercial analog telephone or personal computer. OMNI™ supports secure data communication over analog telephone lines at rates up to 56 Kbps using an integral v.90 modem. This device, which is software upgradable, will offer a higher data rate for digital networks. This terminal is less expensive than a typical STE, and offers interoperability with the STE for data and voice applications. Again, when this device is available, the ARAT will be obtaining several units for testing and configuration for dial-up access into the ARAT SIPRNET network.

These are the technologies that ARAT is currently investigating and will be implementing in the future. These technologies will create more ways for the Warfighter's to access the critical data they need. The current cost per unit is:

- Office STE - $3,250
- Data STE - $2,930

(cont'd next page)

New Technologies (cont'd)

- Palladium Secure Modem - $900
- OMNI™ Secure Terminal - $1,495*

** The first 2000 units purchased throughout the Government will cost $2,385*

Submitted by Mr. Marc C. Demarest, ILEX Systems

The Future of EW Threat Databases - Project K2000

Project K2000 is the National Security Agency's (NSA) upgrade to the Electronic Warfare Integrated Reprogramming database (EWIRDB). Although the EWIRDB is an excellent database, it has some shortfalls. Two problems are that: 1) it is open to personal interpretations, and 2) it is extremely hard to teach the EWIRDB to new Electronic Warfare (EW) personnel or analysts. Anyone, including experienced engineers and analysts that have used EWIRDB, knows that it not user friendly. This leads us to NSA deciding to create Project K2000.

To begin, what is Project K2000? As stated in the K2000 student's guide, "K2000 is the software program used for signals visualization. K2000 is a visualization tool that produces a graphical representation of a signal and presents the underlying signal parameters. What K2000 is not is a database or replacement for KILTING. K2000 has been under development for several years and is still in prototype." So, who is building K2000, and how will it affect the EW community?

The K2000 Project team is made up of individuals from NSA, Scientific and Technical Intelligence (S&TI) Centers, and the EW Community customer organizations. Their goal is to design, develop, and demonstrate a digital/graphical technical Electronic Intelligence production and delivery mechanism in support of the EW community and the Warfighter. As for how it will affect the CECOM's EW community, we at the SEC Electronic Combat Branch (ECB) have just begun investigating K2000's strengths and weaknesses.

Keeping consistent with SEC's efforts in leadership with new technologies, we are proactively working to see how, and if, K2000 can or will be integrated into our Mission Data Set (MDS) simulations and testing cycles. The Electronic Warfare Associates, Inc. (EWA) has been asked by NSA to build and test an Advanced Multiple Environment Simulator (AMES) II plug-in for the Project K2000. This plug-in will allow for the simulation's Database Import Facility (DIF) files to be built directly from the K2000 files and imported into an AMES. If this can be done consistently and without errors, it will tremendously reduce the amount of time devoted to designing test simulations for EW threats. As the MDS programming schedule permits, the ECB will begin beta testing of EWA's AMES plug-in on the AMES II, Micro-AMES II, and the Pico-AMES in SECs Computer Equipment Laboratory (CEL). As with all of the ECB endeavors, the Branch will ensure Project K2000 testing, evaluation and implementation will allow for only the finest software to be fielded, adhering to CECOM's policy of "The Soldier First".

Submitted by Mr. Mike Lewis, ILEX Systems

For Your Information

Coming Events!

Event	*Location*	*Date(s)*
IEW Conference	*Sheraton Eatontown/Pruden Auditorium, Fort Monmouth, NJ*	*15-16 August 2001*
TechNet Fort Monmouth	*Atlantic City, NJ*	*11-14 September 2001*
Command, Control, Communications, Computers and Intelligence Systems Technology	*Fort Huachuca, AZ*	*2-4 October 2001*
AUSA Annual Meeting	*Marriott Wardman Park/Omni Shoreham Hotels, Washington, DC*	*15-17 October 2001*
MILCOM 2001	*Sheraton Premiere @ Tysons Corner, VA*	*28-31 October 2001*
38th Annual AOC International Symposium and Convention	*Omni Shoreham Hotel, Washington, DC*	*28-31 October 2001*

Now Available on the Web

All 22 previous issues of the "ARAT Bulletin" and the "A/IEW Bulletin" are now available on the ARAT web site. The issues are available in HTML format for on-line viewing, as well as in PDF and MS Word 97 format for viewing and downloading.

Future issues will also be posted on the site and in the same format. You are encouraged to download any issue (or issues) for local reproduction and distribution within your agency.

The ARAT web site can be accessed at http://arat.iew.sed.monmouth army.mil/, or from a link on the A/IEW web site at http://www.iew.sed.monmouth.army.mil/

Help Us Help You

If you are moving, have moved, or your address is listed incorrectly on the mailing envelope, please call Ms. Sandra Hoffmann at (732) 530-7766 ext. 338; or email at BulletinUpdates@arat.iew.sed.monmouth.army.mil with the correct address. Many Bulletins are returned for incorrect addresses and unknown addressees. We would like to reduce the amount of returned mail and ensure that all of our customers receive the latest issue of the "A/IEW Bulletin". Thank you for your support.

ARAT Rapid Reprogramming Communications Infrastructure Laboratory (R^2CIL)

Telephone:
#1 (732) 532-9395
DSN: 992-9395
#2 (732) 532-9392
DSN: 992-9392
#3 (732) 532-1859
DSN: 992-1859
#4 (732) 532-5319
DSN: 992-5319 -or-*
(732) 530-7766 ext.: 318 or 324**
** Answering machine/voice mail option available at this number for after-hour messages*

Email:
Unclassified:
webmaster@arat.iew.sed.monmouth.army.mil
SIPRNET:
webmaster@arat.army.smil.mil

ATTENTION ELECTRONIC WARFARE OFFICERS!

Electronic Warfare Officers requiring Memory Loader/Verifier (MLV) reprogramming kits, copies of the "ARAT Software and Documentation Toolbox" CD or the "Mission Data Set Training" CD should contact either Ms. Fanny Leung-Ng (DSN: 312-992-1859/CML: 732-532-1859) (fanny.leung-ng@mail1.monmouth.army.mil) or R^2CIL (DSN: 312-992-9395/9392/CML: 732-532-9395/9392) (webmaster@arat.iew.sed.monmouth.army.mil) or fax your requests to DSN: 312-992-8287/5238 or CML: (732) 532-8287/5238.

The A/IEW Community Key Points of Contact

Agency	Name/e-mail	Comm/DSN	Fax Number
Chief, A/IEW Division	Mr. Joseph Ingrao joseph.ingrao@mail1.monmouth.army.mil	(732) 532-0065 DSN 992-0065	(732) 532-8287 DSN 992-8287
Deputy Chief, A/IEW Division	Dr. Ihor Hapij ihor.hapij@mail1.monmouth.army.mil	(732) 532-8199 DSN 992-8199	(732) 532-5238 DSN 992-5238
Avionics Branch	Mr. Edward Wuyscik edward.wuyscik@mail1.monmouth.army.mil	(732) 427-3924 DSN 987-3924	(732) 427-3923 DSN 987-3923
Electronic Combat Branch ARAT-SE (CECOM)	Mr. Gary Clerie gary.clerie@mail1.monmouth.army.mil	(732) 532-1337 DSN 992-1337	(732) 532-5238 DSN 992-5238
GUARDRAIL Branch	Mr. Raymond Santiago raymond.santiago@mail1.monmouth.army.mil	(732) 532-1420 DSN 992-1420	(732) 532-8287 DSN 992-8287
Intelligence Fusion Branch	Mr. William Walker walker@huachuca-emh27.army.mil	(520) 538-6188 DSN 879-6188	(520) 538-7673 DSN 879-7673
SIGINT Branch	Mr. Robert Hart robert.hart@mail1.monmouth.army.mil	(732) 532-6253 DSN 992-6253	(732) 532-8287 DSN 992-8287
Sensors Branch	Mr. Frank Toth frank.toth@mail1.monmouth.army.mil	(732) 532-8353 DSN 992-8353	(732) 532-8287 DSN 992-8287
ARAT-TA (Eglin AFB)	Mr. Norman Svarrer svarrer@eglin.af.mil	(850) 882-8899 DSN 872-8899	(850) 882-9609 (C) -4268 (U) DSN 872-9609 (C) -4268 (U)
ARAT-TA (Kelly AFB)	SFC Phillip Drake phillip.drake@lackland.af.mil	(210) 977-2021 DSN 969-2021	(210) 977-2145 DSN 969-2145
ARAT-SC (Fort Rucker)	Mr. George Hall hallg@rucker.army.mil	DSN 558-9334	DSN 558-1165

The A/IEW Bulletin Staff

Editor-In-Chief
Mr. Joseph Ingrao, A/IEW Division

Editor
Mr. Joseph Skarbowski, ILEX Systems

Assistant Editor/Distribution Manager
Ms. Sandra Hoffmann, ILEX Systems

Send comments, changes of address, and articles to:
U.S. Army CECOM
Software Engineering Center
ATTN: AMSEL-SE-WS-AI
Fort Monmouth, NJ 07703
FAX: 992-5238 (DSN);
732-532-5238 (Commercial)